00 207
YOR

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２０００年 ７月 ７日

出 願 番 号
Application Number: 特願２０００－２０７５８７

出 願 人
Applicant (s): インターナショナル・ビジネス・マシーンズ・コーポレーション

２００１年 １月１９日

特 許 庁 長 官
Commissioner,
Patent Office 及 川 耕 造

出証番号 出証特２０００－３１１４５７０

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

【書類名】　特許願

【整理番号】　JP9000207

【提出日】　平成12年 7月 7日

【あて先】　特許庁長官殿

【国際特許分類】　G06F 17/60

【発明者】

【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　大和事業所内

【氏名】　豊島　浩文

【発明者】

【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　大和事業所内

【氏名】　田中　唯人

【発明者】

【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　大和事業所内

【氏名】　山下　雄司

【特許出願人】

【識別番号】　390009531

【氏名又は名称】　インターナショナル・ビジネス・マシーンズ・コーポレーション

【代理人】

【識別番号】　100086243

【弁理士】

【氏名又は名称】　坂口　博

【復代理人】

【識別番号】　100112520

【弁理士】

【氏名又は名称】　林　茂則

【電話番号】　　046-277-0540

【選任した代理人】

【識別番号】　　100091568

【弁理士】

【氏名又は名称】　市位　嘉宏

【選任した代理人】

【識別番号】　　100106699

【弁理士】

【氏名又は名称】　渡部　弘道

【選任した復代理人】

【識別番号】　　100110607

【弁理士】

【氏名又は名称】　間山　進也

【選任した復代理人】

【識別番号】　　100098121

【弁理士】

【氏名又は名称】　間山　世津子

【手数料の表示】

【予納台帳番号】　091156

【納付金額】　　21,000円

【提出物件の目録】

【物件名】　　明細書　1

【物件名】　　図面　1

【物件名】　　要約書　1

【包括委任状番号】　9706050

【包括委任状番号】　9704733

【包括委任状番号】　0004480

【プルーフの要否】　　要

【書類名】　　明細書

【発明の名称】　ネットワークシステム、端末管理システム、端末管理方法、データ処理方法、記録媒体およびインターネットサービス提供方法

【特許請求の範囲】

【請求項１】　コンピュータネットワークに接続された端末を端末管理サーバを用いて管理するネットワークシステムであって、

前記コンピュータネットワークに接続された一般管理コンソールと、

前記サーバにアクセス可能な特権管理コンソールと、

前記端末管理サーバに接続されたデータベースと、

前記一般管理コンソールまたは特権管理コンソールと前記データベースとの間のデータ処理を仲介するコンソールマネージャと、を有し、

前記データベースには、前記一般管理コンソール毎に関連付けられている企業データと、前記企業データに関連付けられている前記端末毎の端末データと、を含み、

前記企業データと端末データとを参照して、前記関連付けられている端末またはそのグループに対するサービスの提供を前記関連付けられている一般管理コンソールに対して許可する手段を含む、ネットワークシステム。

【請求項２】　前記データベースには、前記サービスに関連付けられているプロファイルデータを含み、

前記コンソールマネージャには、前記プロファイルデータに関連付けられている前記サービスの登録、変更、スケジューリング、消去その他の前記プロファイルデータに対するアクセスを、前記関連付けられている一般管理コンソールに許可する手段を含む、請求項１記載のネットワークシステム。

【請求項３】　前記データベースには、前記プロファイルデータに関連付けられているジョブデータを含み、

前記端末が前記端末管理サーバに接続した時に、前記ジョブデータを検索し、自己の端末データに関連付けられているサービスの提供を要求する手段を有する請求項２記載のネットワークシステム。

【請求項４】　前記データベースには、さらに前記一般管理コンソール毎に

関連付けられた管理者データを含み、前記一般管理コンソールが前記端末管理サーバにログインする際に、前記企業データおよび管理者データを用いて管理者の認証を行う手段を有する請求項１記載のネットワークシステム。

【請求項５】　全ての前記端末に関連付けられている端末データ、企業データ、管理者データ、プロファイルデータまたはジョブデータへのアクセス、登録、変更および消去を前記特権管理コンソールに許可する手段を含む請求項１記載のネットワークシステム。

【請求項６】　コンピュータネットワークに接続された端末と、前記端末を管理する端末管理サーバと、前記コンピュータネットワークに接続された一般管理コンソールと、前記サーバにアクセス可能な特権管理コンソールと、前記端末管理サーバに接続されたデータベースと、前記一般管理コンソールまたは特権管理コンソールと前記データベースとの間のデータ処理を仲介するコンソールマネージャとを有し、前記データベースには、前記一般管理コンソール毎に関連付けられている企業データと、前記企業データに関連付けられている前記端末毎の端末データと、を含むネットワークシステムにおける端末管理方法であって、

前記一般管理コンソールから前記端末管理サーバに接続要求を発するステップと、

前記コンソールマネージャが、前記一般管理コンソールの企業ＩＤを含む情報を取得し、前記企業データを検索して前記一般管理コンソールに認証を与えるステップと、

前記企業ＩＤで特定された企業データに関連付けられている端末データを有する端末またはそのグループに対するサービスの提供を前記認証された一般管理コンソールに対して許可するステップと、

を含む、端末管理方法。

【請求項７】　前記データベースには、前記サービスに関連付けられているプロファイルデータを含み、

前記認証された一般管理コンソールに対して、前記プロファイルデータに関連付けられている前記サービスの登録、変更、スケジューリング、消去その他の前記プロファイルデータに対するアクセスを許可するステップを有する請求項６記

載の端末管理方法。

【請求項８】　前記データベースには、前記プロファイルデータに関連付けられているジョブデータを含み、

前記端末が前記端末管理サーバに接続するステップと、

前記ジョブデータを検索するステップと、

前記端末の端末データに関連付けられているサービスの提供を要求するステップと、

を有する請求項７記載の端末管理方法。

【請求項９】　前記データベースには、さらに前記一般管理コンソール毎に関連付けられた管理者データを含み、

前記一般管理コンソールが前記端末管理サーバにログインするステップと、

前記企業データおよび管理者データを用いて管理者の認証を行うステップと、

を有する請求項６記載の端末管理方法。

【請求項１０】　全ての前記端末に関連付けられている端末データ、企業データ、管理者データ、プロファイルデータまたはジョブデータへのアクセス、登録、変更および消去が前記特権管理コンソールに許可される請求項６記載の端末管理方法。

【請求項１１】　コンピュータネットワークに接続された端末を管理するシステムであって、

前記コンピュータネットワークに接続された端末管理サーバと、

前記サーバにアクセス可能な特権管理コンソールと、

前記端末管理サーバに接続されたデータベースと、

前記コンピュータネットワークに接続された一般管理コンソールまたは前記特権管理コンソールと前記データベースとの間のデータ処理を仲介するコンソールマネージャと、を有し、

前記データベースには、前記一般管理コンソール毎に関連付けられている企業データと、前記企業データに関連付けられている前記端末毎の端末データと、を含み、

前記一般管理コンソールの要求に応じて、前記企業データと端末データとを参

照し、前記関連付けられている端末またはそのグループに対するサービスの提供を前記関連付けられている一般管理コンソールに対して許可する手段を含む、端末管理システム。

【請求項１２】　前記データベースには、前記サービスに関連付けられているプロファイルデータを含み、

前記コンソールマネージャには、前記プロファイルデータに関連付けられている前記サービスの登録、変更、スケジューリング、消去その他の前記プロファイルデータに対するアクセスを、前記関連付けられている一般管理コンソールに許可する手段を含む、請求項１１記載の端末管理システム。

【請求項１３】　前記データベースには、前記プロファイルデータに関連付けられているジョブデータを含み、

前記端末が前記端末管理サーバに接続した時に、前記ジョブデータを検索し、自己の端末データに関連付けられているサービスの提供を要求する手段を有する請求項１２記載の端末管理システム。

【請求項１４】　前記データベースには、さらに前記一般管理コンソール毎に関連付けられた管理者データを含み、前記一般管理コンソールが前記端末管理サーバにログインする際に、前記企業データおよび管理者データを用いて管理者の認証を行う手段を有する請求項１１記載の端末管理システム。

【請求項１５】　全ての前記端末に関連付けられている端末データ、企業データ、管理者データ、プロファイルデータまたはジョブデータへのアクセス、登録、変更および消去を前記特権管理コンソールに許可する手段を含む請求項１１記載の端末管理システム。

【請求項１６】　コンピュータネットワークに接続された端末を管理する端末管理サーバと、前記サーバにアクセス可能な特権管理コンソールと、前記端末管理サーバに接続されたデータベースと、前記特権管理コンソールまたは前記コンピュータネットワークに接続された一般管理コンソールと前記データベースとの間のデータ処理を仲介するコンソールマネージャとを有し、前記データベースには、前記一般管理コンソール毎に関連付けられている企業データと、前記企業データに関連付けられている前記端末毎の端末データと、を含む端末管理システ

ムを用いたデータ処理方法であって、

前記一般管理コンソールからの接続要求に応じて、前記コンソールマネージャが、前記一般管理コンソールの企業ＩＤを含む情報を取得するステップと、

前記企業データを検索して前記一般管理コンソールに認証を与えるステップと、

前記企業ＩＤで特定された企業データに関連付けられている端末データを有する端末またはそのグループに対するサービスの提供を前記認証された一般管理コンソールに対して許可するステップと、

を含む、データ処理方法。

【請求項１７】　前記データベースには、前記サービスに関連付けられているプロファイルデータを含み、

前記認証された一般管理コンソールに対して、前記プロファイルデータに関連付けられている前記サービスの登録、変更、スケジューリング、消去その他の前記プロファイルデータに対するアクセスを許可するステップを有する請求項１６記載のデータ処理方法。

【請求項１８】　前記データベースには、前記プロファイルデータに関連付けられているジョブデータを含み、

前記端末からの接続要求に応じて、前記端末を接続するステップと、

前記ジョブデータを検索するステップと、

前記端末の端末データに関連付けられているサービスを前記端末に提供するステップと、

を有する請求項１７記載のデータ処理方法。

【請求項１９】　前記データベースには、さらに前記一般管理コンソール毎に関連付けられた管理者データを含み、

前記一般管理コンソールの接続要求に応じて、前記企業データおよび管理者データを用いた前記一般管理コンソールの管理者の認証を行うステップ、

を有する請求項１６記載のデータ処理方法。

【請求項２０】　全ての前記端末に関連付けられている端末データ、企業データ、管理者データ、プロファイルデータまたはジョブデータへのアクセス、登

録、変更および消去が前記特権管理コンソールに許可される請求項１６記載のデータ処理方法。

【請求項２１】　プログラムが記録されたコンピュータ可読な記録媒体であって、

コンピュータネットワークに接続された一般管理コンソールからの接続要求に応じて、前記一般管理コンソールから企業ＩＤを含む情報を取得し、

前記端末管理サーバに接続されているデータベースの企業データを検索して前記一般管理コンソールに認証を与え、

前記企業ＩＤで特定された企業データに関連付けられている前記データベースに記録されている端末データを有する端末またはそのグループを検索し、

前記端末またはそのグループに対するサービスの提供を前記認証された一般管理コンソールに対して許可する機能をコンピュータに実現させるプログラムが記録された記録媒体。

【請求項２２】　前記認証された一般管理コンソールに対して、前記サービスの登録、変更、スケジューリング、消去その他の前記サービスに関連付けられているプロファイルデータに対するアクセスを許可する機能をさらにコンピュータに実現させる請求項２１記載のプログラムが記録された記録媒体。

【請求項２３】　前記端末からの接続要求に応じて、前記端末を接続し、

前記プロファイルデータに関連付けられているジョブデータを検索し、

前記端末の端末データに関連付けられているサービスを前記端末に提供する機能をさらにコンピュータに実現させる請求項２２記載のプログラムが記録された記録媒体。

【請求項２４】　インターネットに接続された第１の端末群に対するサービスを第１の企業に属する第１のコンソールに許可するステップと、

インターネットに接続された第２の端末群に対するサービスを第２の企業に属する第２のコンソールに許可するステップと、

を含むインターネットサービス提供方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、コンピュータネットワークシステムおよびコンピュータネットワークを用いたサービスの提供方法に関し、特に外部ネットワークに接続された端末を特定のグループに分け、そのグループに属する端末を管理する一般管理業務をサポートするシステムに適用して有効な技術に関する。

【０００２】

【従来の技術】

近年、インターネット市場の拡大とその多様化が進展している。インターネットの末端ユーザ（コンシューマ）の要求は、より高い付加価値を求める傾向にある。コンシューマ・ユーザの中にはパーソナル・コンピュータの操作に慣れ親しんだ者ばかりでなく、いわゆる初心者レベルの者も少なくない。このようなユーザにとってはパーソナル・コンピュータへのアプリケーション・ソフトウェアの導入やオペレーティング・システムの詳細な設定作業の負担が大きい。一方、インターネットを用いてサービスを提供しようとする企業にとっては、より魅力的なサービスあるいは付加的なサービスを提供して他企業との差別化を図り、コンシューマ・ユーザの取り込み（裾野の拡大）を図りたいニーズがある。

【０００３】

ところで、ＬＡＮ接続された端末を持つシステムでは、システム管理ツールを用いて端末を管理することができる。システム管理ツールでは端末へのアプリケーション・ソフトウェアの導入、端末の詳細な設定等が行える。このような従来のシステム管理ツールでは、ＬＡＮ接続されていることが前提になり、端末を管理する管理コンソールは管理サーバと同じ企業内等のネットワークに接続されている必要がある。また、システムは一企業内で運用されることが前提であるため、複数の管理コンソールごとに管理対象の端末に対するアクセス管理をするような機能は備えていない。すべての端末を管理できるのが管理コンソールとして一般的である。また、管理コンソールはＬＡＮ接続されていることが前提のため、管理コンソールとサーバ間におけるセキュリティはユーザーIDとパスワードによるユーザー認証のみで行われている。

【０００４】

【発明が解決しようとする課題】

ところが、企業がインターネットを用いて、コンシューマ・ユーザに対し、より高い付加価値を有するサービスを提供しようとした場合、従来技術を前提とすれば、企業は端末を管理する管理コンソールと管理サーバとを自社内に構築した上でインターネットに接続しなければならない。企業は管理システムの初期構築や管理サーバの運用を自社で行わなければならず、特に中小規模の企業にとっては、その負担増加が大きな問題となっている。

【０００５】

一方、そのような企業が既存のネットワークを一部借用してシステムの運用を外部に委託しようとしても、従来技術では複数の管理コンソールごとに管理対象の端末に対するアクセス管理をするような機能が無いため、特定の端末グループを管理対象とする企業のニーズにそぐわない。さらに従来技術では、管理コンソールはLAN接続されていることが前提のため、管理コンソールと管理サーバ間におけるセキュリティはユーザーIDとパスワードによるユーザー認証のみであり、管理コンソールを外部ネットワーク経由でサーバに接続させることは、セキュリティ上問題があった。

【０００６】

本発明の第一の目的は、企業側に管理コンソールのみ設置して面倒な管理サーバの運用から開放できるシステム構成を可能にすることにある。例えば、あるＩＳＰ（インターネット・サービス・プロバイダ）側に端末管理サーバを設置すれば、ＩＳＰは有料で端末管理サービスを複数の企業に対して提供でき、企業側も経費を削減できる効果を期待できる。

【０００７】

第二の目的は、複数の企業が、同じ端末管理サーバやデータベース・サーバを共用して、自社の管理する端末に対してのみソフトウェア配布や端末設定などのサービスが行えるようにする技術を提供することにある。複数コンソールの端末に対するアクセス管理をサポートすることである。より具体的には、この機能によって、他社の端末に対して端末設定などができないようにすることにある。

【０００８】

第三の目的は、管理コンソールと管理サーバー間のセキュリティを強化して外部ネットワークを経由して管理コンソールが使用できるようすることにある。

【０００９】

【課題を解決するための手段】

本願の発明の概略を説明すれば、以下の通りである。本願の発明はコンピュータネットワークに接続された端末を端末管理サーバを用いて管理するネットワークシステムであって、コンピュータネットワークに接続された一般管理コンソールと、サーバにアクセス可能な特権管理コンソールと、端末管理サーバに接続されたデータベースと、一般管理コンソールまたは特権管理コンソールとデータベースとの間のデータ処理を仲介するコンソールマネージャと、を有し、データベースには、一般管理コンソール毎に関連付けられている企業データ、企業データに関連付けられている端末毎の端末データ、を含み、企業データと端末データとを参照して、関連付けられている端末またはそのグループに対するサービスの提供を関連付けられている一般管理コンソールに対して許可する手段を含むものである。

【００１０】

また、前記データベースには、サービスに関連付けられているプロファイルデータを含み、コンソールマネージャにはプロファイルデータに対するアクセスを関連付けられている一般管理コンソールに許可する手段を含む。

【００１１】

また、前記データベースには、プロファイルデータに関連付けられているジョブデータを含み、端末が端末管理サーバに接続した時に、ジョブデータを検索し、自己の端末データに関連付けられているサービスの提供を要求する手段を含む。

【００１２】

また、前記データベースには、さらに一般管理コンソール毎に関連付けられた管理者データを含み、一般管理コンソールが端末管理サーバにログインする際に、企業データおよび管理者データを用いて管理者の認証を行う手段を有する。

【００１３】

なお、全ての端末に関連付けられている端末データ、企業データ、管理者データ、プロファイルデータまたはジョブデータへのアクセス、登録、変更および消去は、特権管理コンソールに許可することができる。

【００１４】

【発明の実施の形態】

以下、本発明の実施の形態を図面に基づいて詳細に説明する。ただし、本発明は多くの異なる態様で実施することが可能であり、本実施の形態の記載内容に限定して解釈すべきではない。なお、実施の形態の全体を通して同じ要素には同じ番号を付するものとする。

【００１５】

以下の実施の形態では、主に方法またはシステムについて説明するが、当業者であれば明らかなとおり、本発明は方法、システムの他、コンピュータで使用可能なプログラムコードが記録された媒体としても実施できる。したがって、本発明は、ハードウェアとしての実施形態、ソフトウェアとしての実施形態またはソフトウェアとハードウェアとの組合せの実施形態をとることができる。プログラムコードが記録された媒体としては、ハードディスク、ＣＤ－ＲＯＭ、光記憶装置または磁気記憶装置を含む任意のコンピュータ可読媒体を例示できる。

【００１６】

システム管理サーバ等の各サーバあるいはユーザ端末には一般的なコンピュータシステムを用いることができる。コンピュータシステムには、中央演算処理装置（ＣＰＵ）、主記憶装置（メインメモリ：ＲＡＭ）、不揮発性記憶装置（ＲＯＭ）等を有し、バスで相互に接続される。バスには、その他コプロセッサ、画像アクセラレータ、キャッシュメモリ、入出力制御装置（Ｉ／Ｏ）等が接続されてもよい。バスには、適当なインターフェイスを介して外部記憶装置、データ入力デバイス、表示デバイス、通信制御装置等が接続される。その他、一般的にコンピュータシステムに備えられるハードウェア資源を備えることが可能なことは言うまでもない。外部記憶装置は代表的にはハードディスク装置が例示できるが、これに限られず、光磁気記憶装置、光記憶装置、フラッシュメモリ等半導体記憶装置も含まれる。データの読み出しのみに利用できるＣＤ－ＲＯＭ等の読み出し

専用記憶装置もデータあるいはプログラムの読み出しに適用する場合には外部記憶装置に含まれる。データ入力デバイスには、キーボード等の入力装置、マウス等ポインティングデバイスを備えることができる。データ入力デバイスにはスキャナ等の画像読み取り装置、音声入力装置も含む。表示装置としては、ＣＲＴ、液晶表示装置、プラズマ表示装置が例示できる。コンピュータシステムには、パーソナルコンピュータ、ワークステーション、メインフレームコンピュータ等各種のコンピュータが含まれる。各コンピュータシステムは、ＬＡＮあるいはインターネットで接続されるがこれに限られない。これら接続に用いられる通信回線は、専用線、公衆回線の何れでも良い。無線回線も勿論適用できる。

【００１７】

各サーバ、コンソールあるいは端末は１つのシステムで実現される必要はなく、複数のシステムで分散的に処理されてもよい。つまり、一部のプログラムをユーザのコンピュータで、一部のプログラムをリモートコンピュータで分散的に処理できる。プログラムで利用されるデータは、それがどのコンピュータに記録されているかは問われない。つまり、データの所在に関する情報（アドレス）が明らかでありそのデータが利用可能である限り、データあるいはプログラムの格納場所はコンピュータネットワーク上の任意の場所とすることができる。各ネットワークコンピュータ間の通信には公知の通信技術を適用でき、たとえばＴＣＰ／ＩＰ、ＨＴＴＰ等のプロトコルを用いることができる。また、各記憶装置に記録された各ファイル（データあるいはプログラム）の存在箇所（アドレス）は、ＤＮＳ、ＵＲＬ等を用いて特定できる。なお、本明細書においてインターネットという用語には、イントラネットおよびエクストラネットも含むものとする。インターネットへのアクセスという場合、イントラネットやエクストラネットへのアクセスをも意味する。

【００１８】

１．システム構成

図１は、本実施の形態のネットワークシステムの概要を示した図である。図２は、本実施の形態のシステムを機能に着目してさらに詳細に示した図である。

【００１９】

本実施の形態のネットワークシステムは、ＩＳＰ（インターネット・サービス・プロバイダ）１側に設置される端末管理サーバ２、コンソール・マネージャ３、特権管理コンソール４、ＤＭＳ（デバイス・マネージメント・サーバ）データベース５、アプリケーションサーバ６、ＰＣ（パーソナル・コンピュータ）プラグイン７、および外部ネットワーク８経由で企業側に設置される一般管理コンソール９、および端末管理サービスを受けるクライアント端末１０側に設置されるデバイス・エージェント１１を有する。

【００２０】

ＩＳＰ１は、本実施の形態の端末管理サービスを提供する事業主である。端末管理サーバ２は、認証用のＨＴＴＰサーバ６、ウェブ制御用のアプリケーションサーバ１３、ＰＣプラグイン７、デバイスマネージメントサーブレット１４、ＡＰＩ１２、コンソールマネージャ３、インテグレーションツールキット１７を含む。

【００２１】

コンソール・マネージャ３は、各企業に配られる一般管理コンソール９および特権管理コンソール４からのリクエストを受け付け、アクセス制御を行いながらデータベース５に対する操作を仲介する。

【００２２】

特権管理コンソール４は、ＩＳＰ１側に設置された管理コンソールであり、一般管理コンソール９の登録等の管理を行う。特権管理コンソール４からは、企業ごとに割り当てられる企業IDや管理者IDを管理する。特権管理コンソール４は各端末１０の管理も行える。

【００２３】

データベース５には、一般管理コンソール９の管理に必要なコンソールマネージメントデータベース２０、端末１０の管理に必要なデバイスマネージメントデータベース１９、およびジョブ管理に必要なジョブデータベース１８が収められている。データベース５への操作はＡＰＩ１２を介して行われる。 ＡＰＩ１２には、ジョブＡＰＩ２１、デバイスマネージメントＡＰＩ２２が含まれる。

【００２４】

一般管理コンソール９は各企業に設置されるもので、各企業の管理者は自社管理下のクライアント端末１０に対して、端末管理サービスを実行する。

【００２５】

コンソール・マネージャ３はHTTPサーバ上のサーブレット１４，１５ありで、管理コンソール４，９からの要求はHTTPリクエストの形で受け付けられる。処理結果はHTTPレスポンスの形で返される。管理コンソール４，９とコンソール・マネージャ３間の通信にはSSLのクライアント認証を必要とし、クライアント側の処理はコンソールのSSLライブラリで行う。サーバ４側のSSLの処理は、たとえばアプリケーションサーバ６によって行われる。コンソール・マネージャ３には、DMSデータベース５に追加されたテーブル群(コンソールマネージメントデータベース)とそのテーブル群にアクセスするためのモジュール(コンソールマネージャビジネスオブジェクツ１６)を含む。

【００２６】

また、本願のネットワークシステムでは、SSLによる端末認証が行われた後に、コンソール４，９のログイン時に管理者認証が行われる。管理者認証はコンソール４，９を使用しようとしている人が正規に登録されている管理者かどうかを認証する機能である。コンソール・マネージャ３は認証されていない管理者からの要求は拒否する。認証に必要な入力項目は、たとえば管理者ID、管理者パスワード、企業IDである。ただし、企業IDは企業別に配布されたIDファイルから自動的に読み取られる。

【００２７】

管理者認証はデータベース５のENTERPRISEテーブルとADMINISTRATORテーブルを参照することにより行う。管理者が認証された場合、コンソール・マネージャ３は企業IDと管理者IDをセッションに関連づけて保存し、コンソール４，９に処理の成功を通知する。以降のコンソールからの要求に対しては、前記セッションへ関連づけられたIDをチェックすることにより正当性をチェックすることができる。これによりデータベース・リソースへのアクセス制御可能になる。アクセス権限は企業単位であり、認証は同じセッションの間有効である。認証に失敗した場合および認証されていない人から要求の場合には、コンソール・マネージャ３

はセッションを終了し通信を切断する。なおセッション管理は、管理コンソール４，９に対してログオン時に期限付き認証チケットを発行し以後その認証チケットをセッションIDとして使用することで行うことができる。

【００２８】

データベース５に登録されたサービスは、端末１０に配布される。配布は端末１０がＩＳＰ１のＤＭＳ２に接続した段階でプル型で提供される。すなわち、端末１０は、端末ごとに関連付けられているジョブ・マネージメント・データベースを検索し、自己に登録されているサービスをダウンロードすることによりサービスを受ける。サービスのダウンロードはＰＣプラグイン７とＰＣデバイスエージェント１１を介して行われる。

【００２９】

このようなシステム構成とすることにより、企業は自前のシステムを用意することなく自己の管理する端末に端末サービスを提供できる。また、企業は一般管理コンソールから自己の管理できる端末に対し、システムの用意したサービスに加えて独自のサービスを付加することができる。一方、システム提供者（事業主）は一般の端末ユーザのみならず企業の利用を促すことができ、この企業を介しての端末ユーザの獲得を促進できる。端末ユーザは本システムを利用して付加的なサービスを受けることができる。

【００３０】

２．データベース構成

次に、本システムのコンソールマネージャ用のデータベース２０の構造について説明する。コンソールマネージャ３と、そのデータベース２０は、特権管理コンソール４および一般管理コンソール９を制御するように構成される。企業および管理者は、事業主や特権管理者を含め、このデータベース２０にて管理される。各企業の管理者がコンソール・マネージャ３に要求を出すためにはログオン時に認証されることを必要とする。このように端末管理のみならず管理者の認証を行うことにより、システムのセキュリティを向上できる。

【００３１】

認証後は他の企業のリソースにアクセスできないようにコンソール・マネージ

ャ３によりアクセス制御されながら、管理者の仕事をおこなうことができる。但し特権管理者はこの限りではない。

【００３２】

次に本システムのコンソールマネージャ用のデータベース２０について説明する。図３は、コンソールマネージャ用のデータベース構造を示す図である。

【００３３】

本システムにおいては、端末ユーザのデバイス（端末１０）を企業ごとのグループに区分できる。また、各端末は、その端末が受けることができるサービスごとにグループ化できる。すなわち、１つの端末１０は１つの企業に管理され、１つの端末は１つのサービス・グループに属する。端末１０は同じ企業に管理され同じサービス・グループに属する限りグループ化でき、１つの端末は複数の端末グループに属すことがでる。このような関係を図４に概念的に示す。図４は端末（デバイス）とサービスのグループ関係を示した図である。

【００３４】

サービス・グループとはサービスを組にしたものである。端末が登録されるとその端末は必ずどこかのサービス・グループに属する。端末がサービス・グループに属しているということはその端末がそのサービス・グループ内のサービスを受ける能力のあるものであることを意味する。つまり、サービス・グループはあるサービス群を提供することのできる端末の集合を間接的に表わす。サービス・グループは特権管理者によって設定される。あるサービス・グループを複数の企業それぞれに同時に設定することはできるが、企業間を跨って設定することはできない。データベース２０は以上のグループ管理を行うように構成される。

【００３５】

また、本願の端末管理サーバ(Device Management Server: DMS)のジョブは端末単位に行う。このため、端末グループに対するジョブをサポートするためにジョブのグループ化が必要となる。データベース２０はグループ化されたジョブを管理する。

【００３６】

また、企業の管理者が作成するジョブ・プロファイルはこのデータベース２０

で管理される。サービスという概念は最終的にジョブというDMSの概念にマップされる。ジョブ・プロファイルにはジョブ内容が記述され、各サービスに対応づけられる。

【００３７】

以下にコンソール・マネージャ用データベース２０のテーブル構成を説明する。端末管理サーバ(Device Management Server: DMS)との親和性を考慮して、端末管理サーバの標準テーブル構成を補完する形で設計されている。図３中の「Device Management DB」および「Job Management DB」は端末管理サーバが管理するデータベースである。データベース２０内の各テーブルの詳細は以下のとおりである。

【００３８】

２－１．ENTERPRISEテーブル

ENTERPRISEテーブルは企業のリストを保持する。ENTERPRISEテーブルの一例を表１に示す。各フィールドの詳細は以下のとおりである。

【００３９】

【表１】

Name	Type	Size	Required	Example
ENTERPRISE_ID (PK)	integer	---	Y	1000
ENTERPRISE_SIG	varchar	64	Y	"J0001"
ENTERPRISE_NAME	varchar	255	Y	"日本ABC株式会社"
SUPERVISOR	char	1	Y	'Y'

ENTERPRISE_ID：各企業に対応する内部ID番号である。主にデータベースの内部処理で使用される。特権管理者が企業エントリーを作成・登録する際に自動生成

される。ENTERPRISEテーブル内で唯一になる。

ENTERPRISE_SIG：企業の識別名である。ENTERPRISEテーブル内で唯一である必要がある。特権管理者により各企業に割り当てられる。

ENTERPRISE_NAME：企業の名前である。ENTERPRISEテーブル内で唯一である必要がある。

SUPERVISOR：企業が事業主であるかどうかを表わす。’Y’という文字は事業主、それ以外は一般企業をあらわす。複数の企業が事業主になることはできない。

【００４０】

２－２．ADMINISTRATORテーブル

ADMINISTRATORテーブルは管理者のリストを保持する。ADMINISTRATORテーブルの一例を表２に示す。各フィールドの詳細は以下のとおりである。

【００４１】

【表２】

Name	Type	Size	Required	Example
ADMIN_ID (PK)	integer	---	Y	1000
ADMIN_UID	varchar	64	Y	"ichiro"
ADMIN_PASSWORD	varchar	255	Y	(binary)
ADMIN_INFO	varchar	512	N	"特許 一郎 Tel/Fax: 045-123-4567"
ENTERPRISE_ID (FK)	integer	---	Y	1000

ADMIN_ID：各管理者に対応する内部ID番号である。主にデータベースの内部処理で使用される。特権管理者が管理者エントリーを作成・登録する際に自動生成さ

れる。ADMINISTRATORテーブル内で唯一になる。

ADMIN_UID：管理者の識別名である。ADMINISTRATORテーブル内で唯一である必要がある。

ADMIN_PASSWORD：管理者のパスワードである。一方向性ハッシュ関数に通す等の処理を施した平文でないものを格納する。

ADMIN_INFO：管理者の情報である。

ENTERPRISE_ID：管理者が所属している企業を表わす。ENTERPRISEテーブル内のENTERPRISE_IDを指している。所属している企業が事業主の場合、管理者は特権管理者となる。

【００４２】

２－３．SERVICEテーブル

SERVICEテーブルはサービスのリストを保持する。 SERVICEテーブルの一例を表３に示す。各フィールドの詳細は以下のとおりである。

【００４３】

【表３】

Name	Type	Size	Required	Example
SERVICE_ID (PK)	integer	---	Y	1000
SERVICE_SIG	varchar	64	Y	"INTERNET_BUTTON_SETTING"
DEVICE_CLASS_NAME	varchar	256	Y	"PC Type 1"

SERVICE_ID：各サービスに対応する内部ID番号である。主にデータベースの内部処理で使用される。特権管理者がサービス・エントリーを作成・登録する際に自

動生成される。SERVICEテーブル内で唯一になる。

SERVICE_SIG：サービスの識別名である。SERVICE_SIGとDEVICE_CLASS_NAMEの組み合わせは、SERVICEテーブル内で唯一である必要がある。

DEVICE_CLASS_NAME：デバイスクラス名である。デバイスクラスはＰＣプラグインの一部であり、端末との通信をつかさどる。

【００４４】

２－４．SERVICE_GROUPテーブル

SERVICE_GROUPテーブルはサービス・グループのリストを保持する。 SERVICE_GROUPテーブルの一例を表４に示す。各フィールドの詳細は以下のとおりである。

【００４５】

【表４】

Name	Type	Size	Required	Example
SERVICE_GROUP_ID (PK)	integer	---	Y	1000
SERVICE_GROUP_SIG	varchar	64	Y	"SERVICE_GROUP_1"

SERVICE_GROUP_ID：各サービス・グループに対応する内部ID番号である。主にデータベースの内部処理で使用される。特権管理者がサービス・グループを作成・登録する際に自動生成される。SERVICE_GROUPテーブル内で唯一になる。

SERVICE_GROUP_SIG：サービス・グループの識別名である。SERVICE_GROUPテーブル内で唯一である必要がある。

【００４６】

２－５．GROUPED_SERVICESテーブル

GROUPED_SERVICESテーブルはサービスとサービス・グループを関連づける。GROUPED_SERVICESテーブルの一例を表５に示す。

【００４７】

【表５】

Name	Type	Size	Required	Example
SERVICE_ID (FK)	integer	---	Y	1000
SERVICE_GROUP_ID (FK)	integer	---	Y	1000

SERVICE_ID：SERVICEテーブル内のSERVICE_IDを指す。SERVICE_IDとSERVICE_GRO
UP_IDの組み合わせはGROUPED_SERVICESテーブル内で唯一である。

SERVICE_GROUP_ID：SERVICE_GROUPテーブル内のSERVICE_GROUP_IDを指す。

【００４８】

２－６．JOB_PROFILEテーブル

JOB_PROFILEテーブルはジョブ・プロファイルのリストを保持する。一例を表６に示す。

【００４９】

【表６】

Name	Type	Size	Required	Example
JOB_PROFILE_ID (PK)	integer	---	Y	1000
JOB_PROFILE_NAME	varchar	255	Y	"桜吹雪アイコン配布"
JOB_PROFILE_CONTENTS	varchar	1024	Y	"file:///jobres/J001/1000/cherrydist.pkg"
JOB_PROFILE_INFO	varchar	512	N	春用アイコンを配布するための・・・
SW_ID	long	---	N	1000000
SERVICE_ID (FK)	integer	---	Y	1000
ENTERPRISE_ID (FK)	integer	---	Y	1000
LAST_MODIFIED	date	---	Y	(date and time)

JOB_PROFILE_ID：各ジョブ・プロファイルに対応する内部ID番号である。主にデータベースの内部処理で使用される。ジョブ・プロファイルのエントリーを作成

・登録する際に自動生成される。JOB_PROFILEテーブル内で唯一である必要がある。

JOB_PROFILE_NAME：ジョブ・プロファイルの名前である。JOB_PROFILE_NAMEとENTERPRISE_IDの組み合わせはJOB_PROFILEテーブル内で唯一である必要がある。

JOB_PROFILE_CONTENTS：ジョブ・プロファイルの内容である。たとえば、ジョブで使用するパッケージファイルのURLが格納される。

JOB_PROFILE_INFO：ジョブ・プロファイルの情報である。このフィールドへの設定は任意である。

SW_ID：DMSのSOFTWAREテーブル中のSW_IDを指す。

SERVICE_ID：SERVICEテーブル内のSERVICE_IDを指す。

ENTERPRISE_ID：ジョブ・プロファイルを持つ企業をあらわす。ENTERPRISEテーブル内のENTERPRISE_IDを指す。

LAST_MODIFIED：ジョブ・プロファイルの最終更新日時である。

【００５０】

２－７．JOB_GROUPテーブル

JOB_GROUPテーブルはジョブ・グループのリストを保持する。一例を表７に示す。

【００５１】

【表７】

Name	Type	Size	Required	Example
JOB_GROUP_ID (PK)	long	---	Y	1000
JOB_GROUP_NAME	varchar	255	Y	"落水さんのラインへのアイコン配布"
JOB_GROUP_INFO	varchar	512	N	"大和1階、大和2階"
JOB_PROFILE_ID (FK)	integer	---	Y	1000
SUBMITTED_TIME	date	---	Y	(date and time)
ACTIVATION_TIME	date	---	Y	(date and time)
EXPIRATION_TIME	date	---	Y	(date and time)
ENTERPRISE_ID (FK)	integer	---	Y	1000
LAST_MODIFIED	timestamp	---	Y	(date and time)

JOB_GROUP_ID：各ジョブ・グループに対応する内部ID番号である。主にデータベースの内部処理で使用される。特権管理者がジョブ・グループエントリーを作成

・登録する際に自動生成される。JOB_GROUPテーブル内で唯一である必要がある。

JOB_GROUP_NAME：ジョブ・グループの名前である。JOB_GROUP_NAMEとENTERPRISE_IDの組み合わせはJOB_GROUPテーブル内で唯一である必要がある。

JOB_GROUP_INFO：ジョブ・グループの情報である。ジョブの実行対象等の情報を格納しておく。このフィールドへの設定は任意である。

JOB_PROFILE_ID：スケジュールされたジョブ内容を表わすものとして、JOB_PROFILEテーブル内のJOB_PROFILE_IDを指す。

SUBMITTED_TIME：ジョブが登録された日時である。

ACTIVATION_TIME：ジョブが実行可能になる日時である。

EXPIRATION_TIME：ジョブが期限切れになる日時である。

ENTERPRISE_ID：ジョブ・グループが属する企業をあらわす。ENTERPRISEテーブル内のENTERPRISE_IDを指す。

LAST_MODIFIED：ジョブ・グループの最終更新日時である。

【００５２】

２－８．SUBMITTED_JOB_EXTテーブル

SUBMITTED_JOB_EXTテーブルはジョブとジョブ・グループを関連づける。一例を表８に示す。

【００５３】

【表８】

Name	Type	Size	Required	Example
JOB_ID (PK, FK)	integer	---	Y	1000
JOB_GROUP_ID (FK)	integer	---	Y	1000

JOB_ID：DMSのSUBMITTED_JOBSテーブル内のJOB_IDを指す。JOB_IDとJOB_GROUP_IDの組み合わせはGROUPED_JOBSテーブル内で唯一である。

JOB_GROUP_ID：JOB_GROUPテーブル内のJOB_GROUP_IDを指す。

【００５４】

２－９．DEVICE_EXTテーブル

DEVICE_EXTテーブルはDMSのDEVICEテーブルに対しての補足情報を保持する。一例を表９に示す。

【００５５】

【表９】

Name	Type	Size	Required	Example
DEVICE_ID (PK, FK)	long	---	Y	1000
N_VALUE	varchar	32	N	"123-4567"
SERVICE_GROUP_ID (FK)	integer	---	Y	1000
ENTERPRISE_ID (FK)	integer	---	Y	1000

DEVICE_ID：DMSのDEVICEテーブル内のDEVICE_IDを指す。DEVICE_EXTテーブル内で唯一である必要がある。

N_VALUE：事業主の管理する端末管理用番号である。

SERVICE_GROUP_ID：端末グループが属するサービスをあわらす。SERVICE_GROUPテーブル内のSERVICE_GROUP_IDを指す。

ENTERPRISE_ID：端末グループが属する企業をあらわす。ENTERPRISEテーブル内のENTERPRISE_IDを指す。

【００５６】

２－１０．DEVICE_GROUPテーブル

DEVICE_GROUPテーブルは端末グループのリストを保持する。一例を表１０に示す。

【００５７】

【表１０】

Name	Type	Size	Required	Example
DEVICE_GROUP_ID (PK)	long	---	Y	1000
DEVICE_GROUP_NAME	varchar	255	Y	"ABC社Y事業所B館6階SE7"
DEVICE_GROUP_INFO	varchar	512	N	大和市下鶴間・・・
SERVICE_GROUP_ID (FK)	integer	---	Y	1000
ENTERPRISE_ID (FK)	integer	---	Y	1000
LAST_MODIFIED	date	---	Y	(date and time)

DEVICE_GROUP_ID：各端末グループに対応する内部ID番号である。主にデータベースの内部処理で使用される。特権管理者が端末グループエントリーを作成・登

録する際に自動生成される。DEVICE_GROUPテーブル内で唯一になる。

DEVICE_GROUP_NAME：端末グループの名前である。DEVICE_GROUP_NAMEとENTERPRISE_IDの組み合わせはDEVICE_GROUPテーブル内で唯一である必要がある。

DEVICE_GROUP_INFO：端末グループの情報である。このフィールドへの設定は任意である。

SERVICE_GROUP_ID：端末グループが属するサービスをあわらす。SERVICE_GROUPテーブル内のSERVICE_GROUP_IDを指す。

ENTERPRISE_ID：端末グループが属する企業をあらわす。ENTERPRISEテーブル内のENTERPRISE_IDを指す。

LAST_MODIFIED：端末グループの最終更新日時である。

【００５８】

２－１１．GROUPED_DEVICESテーブル

GROUPED_DEVICESテーブルは端末と端末グループを関連づける。一例を表１１に示す。

【００５９】

【表１１】

Name	Type	Size	Required	Example
DEVICE_ID (FK)	long	---	Y	1000
DEVICE_GROUP_ID (FK)	long	---	Y	1000

DEVICE_ID：DMSのDEVICEテーブル内のDEVICE_IDを指す。DEVICE_IDとDEVICE_GRO
UP_IDの組み合わせはGROUPED_DEVICESテーブル内で唯一である。
DEVICE_GROUP_ID：DEVICE_GROUPテーブル内のDEVICE_GROUP_IDを指す。

【００６０】

以上の各テーブルを有するデータベースを構成して、前記したシステムを稼動できる。なお、前記各テーブルの要素には任意な要素が含まれ、それら要素は本発明の必須の要件ではない。また、他の任意な要素を付加できることは勿論である。

【００６１】

３．システムの機能

次に、本システムが実現する機能を説明する。図５は、特権管理コンソールから端末管理サーバにリクエストを出し、サーバがこのリクエストに応える場合の処理の手順を示した図である。図中左側にコンソール側の処理要求を記し、右側に管理サーバ（コンソールマネージャ）の処理内容を記している。また、図６は、一般管理コンソールから端末管理サーバにリクエストを出し、サーバがこのリクエストに応える場合の処理の手順を示した図である。図中左側にコンソール側の処理要求を記し、右側に管理サーバ（コンソールマネージャ）の処理内容を記している。また、図７は、エンドユーザの端末から端末管理サーバにリクエストを出し、サーバがこのリクエストに応える場合の処理の手順を示した図である。図中左側に端末側の処理要求を記し、右側に管理サーバ（デバイスマネージャ）の処理内容を記している。

【００６２】

なお本システムの機能の実現において、管理コンソールからの通信内容は以下の２種類に大別される。第１にコンソール・マネージャへのデータベース検索・更新要求(コマンド)であり、第２に端末へ配布するファイルのアップロードである。前者はXMLベースのやりとりで行なうことができ。後者はHTMLのPOSTコマンドを使用することができる。XML上に定義する書式とその内容、およびPOSTコマンドの利用によるファイルのアップロード等、詳細は当業者に公知である。また、本システムの通信においては、データ圧縮、NLSへの対応、巨大なデータの分割送信(受信)と部分再送信(受信)機能、各企業の持つ私的情報(管理者パスワード等)の暗号化等の機能を付加することができる。

【００６３】

以下、各コンソールまたは端末と管理サーバとの間の処理の詳細を説明する。

【００６４】

３-１．管理者認証

管理者認証は、特権管理または一般管理コンソールを使用しようとしている人が正規の登録されている管理者かどうかを認証する機能である。コンソール・マネージャは認証されていない管理者からの要求は受け付けない。特権管理コンソール４または一般管理コンソール９がログインすると（ステップ３０）、コンソールは設定ファイル内の企業ＩＤとログイン時に入力された管理者ＩＤおよびパスワードをサーバ２（コンソールマネージャ３）に送付する（ステップ３１）。通信はＳＳＬハンドシェイクで行う。コンソールマネージャ３は正当性のチェック（認証）を行い（ステップ３２）、ログインレスポンスを返す（ステップ３３）。

【００６５】

管理者認証はデータベースのENTERPRISEテーブル３４とADMINISTRATORテーブル３５を参照することによりおこなう。管理者が認証された場合、コンソール・マネージャは企業IDと管理者IDをセッションに関連づけて保存し、コンソールに処理の成功を通知する（ステップ３３）。以降のコンソールからの要求に対しては、前述のセッションへ関連づけられたIDをチェックすることにより正当性をチェックすることができる。これによりリソースへのアクセス制御可能になる。アクセス権限は企業単位である。認証は同じセッションの間有効である。認証に失敗した場合、および認証されていない人からの要求の場合には、コンソール・マネージャはセッションを終了し通信を切断する。なおセッション管理は、管理コンソールに対してログオン時に期限付き認証チケットを発行し、以後その認証チケットをセッションIDとして使用することでおこなえる。

【００６６】

３-２．企業の管理

企業の管理は特権管理コンソールからのみ行える（特権操作）。コンソールマネージャは特権管理コンソールからのリクエストであるか否かを特権フラグが「true」であるか否かで判断する。特権フラグはログインレスポンスの際にコンソ

ールに送付される。

【００６７】

企業の追加（ステップ３６）は、コンソールからの企業追加リクエスト３７に応答して、コンソールマネージャがENTERPRISEテーブル３４にエントリーを追加することによりおこなう（ステップ３８）。事業主の企業はあらかじめ導入時にプリセットされ、事業主の追加はできない。企業識別名は各企業の管理者に配布するものとデータベースにセットされるものが一致していなければならない。追加処理の後、コンソールマネージャは特権管理コンソールにＯＫのレスポンスを返す（ステップ３９）。

【００６８】

企業の削除は、ENTERPRISEテーブルからエントリーを削除することによりおこなう。企業を削除する際には、その企業に関連づけられている管理者、端末グループ、端末、ジョブグループ、ジョブ、ジョブ・プロファイル等もすべて削除されている必要がある。なお、事業主の企業の削除はできない。企業属性の変更はENTERPRISEテーブルのエントリーを変更することによりおこなう。なお、企業のリストはENTERPRISEテーブルを参照することによりおこなえる。

【００６９】

３－３．管理者の管理

管理者の管理は、企業管理と同様に特権操作である。但し一部は一般管理者にも許可される。

【００７０】

管理者の追加（ステップ４０）はADMINISTRATORテーブルにエントリーを追加することによりおこなう。前記と同様にリクエストをサーバに送付し、サーバ（コンソールマネージャ）がリクエストに応答してデータベースを書き換えることにより行う。最低一人の特権管理者は導入時にあらかじめプリセットされている。

【００７１】

管理者の削除はADMINISTRATORテーブルからエントリーを削除することによりおこなう。特権管理者が一人もいなくなるような削除操作はできない。

【００７２】

管理者属性の変更はADMINISTRATORテーブルのエントリーを変更することによりおこなう。特権管理者は任意の管理者の管理者パスワードと管理者情報を変更できる。一般管理者は自身の管理者パスワードの変更しかできない。

【００７３】

管理者のリストはADMINISTRATORテーブルとENTERPRISEテーブルを参照することによりおこなう。

【００７４】

３－４．企業の切り替え

特権管理コンソールからのリクエストに応じて、コンソールマネージャは企業ＩＤを変更して企業の切り替えを行える（ステップ４１）。

【００７５】

３－５．端末管理

端末管理は原則として特権管理であるが、一部は一般管理者にも許可される。

【００７６】

端末の追加（ステップ４２）は特権操作である。端末の追加はDMS上のDEVICEテーブル（デバイスマネージメントデータベース１９内に記録される）にエントリーを追加し、同時にDEVICE_EXTテーブル４４にも対応するエントリーを追加することによりおこなう。

【００７７】

端末の削除も特権操作である。端末の削除はDMS上のDEVICEテーブルからエントリーを削除すると同時に、DEVICE_EXTテーブルからも対応するエントリーを削除することによりおこなう。

【００７８】

端末属性の変更（特権操作)は、DMS上のDEVICEテーブルまたはDEVICE_EXTテーブルのエントリーを変更することによりおこなう。

【００７９】

端末リストはDMS上のDEVICEテーブル、DEVICE_EXTテーブル、GROUPED_DEVICESテーブルを参照しておこなう。ある端末グループに属する全端末をリストできる

【００８０】

端末のグループ化はGROUPED_DEVICESテーブルにエントリーを追加することによりおこなう。グループ化される端末は、同じ企業かつ同じサービス・グループに属していることが必要になる。まず端末グループを作ってから端末をリストし、グループ化する。

【００８１】

なお、サービスグループは、端末のグループ化を考える上で必要な概念である。サービス・グループには２つの側面がある。１つは事業主が各企業に対して提供するサービスの枠組(下地)をあらわすものという見方である。たとえば、サービス１とサービス２を持つサービス・グループを事業主が設定し、各企業はサービス１とサービス２に対してそれぞれ独自の内容をのせ込むことができる。もう一つの側面は、端末をサービス・グループに関連づけることにより、ある端末がサービス・グループに含まれるサービス群を受ける能力があることを保証しているという見方である。

【００８２】

３－６．端末グループ管理

端末グループの追加はDEVICE_GROUPテーブルにエントリーを追加することによりおこなう。端末グループの削除はDEVICE_GROUPテーブルからエントリーを削除することによりおこない、同時にGROUPED_DEVICESテーブル中の対応するエントリーもすべて削除する。端末グループ属性の変更はDEVICE_GROUPテーブルのエントリーを変更することによりおこない、変更可能な属性は端末グループ名のみである。端末グループのリストはDEVICE_GROUPテーブルとGROUPED_DEVICESテーブルを参照することによりおこなう。ある端末が属している全端末グループをリスト、或いはある端末グループに属している全端末をリストすることができる。

【００８３】

３－７．ジョブ管理

コンソールとコンソール・マネージャにおいて、サービスはジョブというDMS上の概念にマップされる。DMSでは１端末につき１つのジョブが作られる。ジョ

ブのスケジュールは、端末単位または端末グループ単位でおこなうことができる。いずれの場合にも端末単位にまで分解され、端末の重複を排除し、端末群へのジョブのまとまり(ジョブ・グループ)としてJOB_GROUPテーブルに１つエントリーが追加される。以後、その端末群へのジョブはジョブ・グループ名で参照される。SUBMITTED_JOB_EXTテーブルは、DMSのSUBMITTED_JOBテーブルとジョブ・グループを対応づける。DMS上のSUBMITTED_JOBSテーブルとJOB_PARMSテーブルのフィールドには必要な値がセットされる。

【００８４】

ジョブのキャンセルはジョブ・グループ単位でおこなう。個々の端末へのジョブの単位でもキャンセルできる。ジョブがキャンセルされるとデータベース上から対応するエントリーが削除される。なお、DMSにおけるジョブの削除操作はデータベースからエントリーを削除するのみであり、実行中のジョブそのものに関してはなにも対処されない。ジョブ属性の変更はDMS上のSUBMITTED_JOBテーブルを変更することによりおこなう。

【００８５】

ジョブのリストはDMS上のSUBMITTED_JOBテーブル、JOB_COMPLETIONテーブル、およびSUBMITTED_JOB_EXTテーブル、JOB_GROUPテーブルを参照しておこなう。あるジョブ・グループに属する全ジョブのステータスが取得できる。この場合、ステータスと期日でフィルターをかけることができ、あるジョブが属しているジョブ・グループのリストを取得できる。

【００８６】

３－８．ジョブプロファイルの管理

ジョブ・プロファイルの追加はJOB_PROFILEテーブルにエントリーを追加することによりおこなう。ジョブ・プロファイルを追加する際には、関連するソフトウェアのアップロードをおこない、その情報をDMS上のSOFTWAREテーブルに登録しておく必要がある。ソフトウェアのアップロードはコンソールマネージャのサーブレットが処理する。

【００８７】

ジョブ・プロファイルの削除はJOB_PROFILEテーブルからエントリーを削除す

ることによりおこなう。関連するソフトウェアの削除、SOFTWAREテーブル上の対応するエントリーの削除も同時におこなわれる。なお、あるJOB_PROFILEにより発行されたジョブがデータベース上に存在する場合、そのジョブ・プロファイルは削除できない。

【００８８】

ジョブ・プロファイル属性の変更はJOB_PROFILEテーブルのエントリーを変更することによりおこなう。変更可能な属性はジョブ・プロファイル名のみである。ジョブ・プロファイルのリストはJOB_PROFILEテーブルとSERVICEテーブルを参照することによりおこなう。

【００８９】

３－９．ジョブリソースのアップロード

端末に配布されるソフトウェア等はジョブのスケジュールに先立ちあらかじめアップロードされている必要がある。コンソール・マネージャは管理コンソールからのジョブ・リソースのアップロード要求を処理する。ジョブ・リソースには、たとえば、配布されるソフトウェア(画像、文書、プログラム等)、配布するソフトウェアや設定を記述したパッケージ定義ファイル、上記のものをひとまとめにしたパッケージ、等がある。

【００９０】

図６に示すように、企業側でパッケージファイルを作成し（ステップ４５）、タスク・テンプレートの作成要求（ステップ４６）に応じて、企業ごとにアップロード用ディレクトリが設定される（ステップ４７）。各企業は自分のディレクトリにのみコンソール・マネージャの管理の下でアクセス可能である。アップロード先は例えば以下のようなディレクトリになる。

【００９１】

/jobres/J001

ここで、「/jobres」はすべての企業リソース用ディレクトリの親ディレクトリである。このディレクトリ名を含め、上記のような企業のリソース用ディレクトリへのパスはコンソールマネージャサーブレットがデータベースから得られる識別名等を基に設定する。DMS側のサーバ構成が複数台にわたる時は、「/jobres」

以下は適切に他のマシンにNFSマウントされる必要がある。

【００９２】

コンソール側から前記したディレクトリにパッケージファイル、リソースファイルをアップロードする（ステップ４８）、サーバ側では、タスク・テンプレート・コミット要求（ステップ４９）に応じてこれを作成し（ステップ５０）、JOB_PROFILEテーブルに記録する。

【００９３】

３－１０．端末からのリクエスト処理

図７に示すように、端末からDMSのデバイスマネージャにジョブ有無の問い合わせ（ステップ５１）を行い、サーバはジョブ有無の通知を行う（ステップ５２）。ジョブがなければここで処理を終了する。ジョブが有る場合には、ジョブ情報の送信要求を端末が発し（ステップ５３）、要求に応じてサーバはジョブ情報を通知する（ステップ５４）。ジョブの開始要求（ステップ５５）に応じて、サーバはジョブの開始通知を発し（ステップ５６）、端末から継続要求があれば、サーバはジョブが終了するまでジョブを実行する（ステップ５７）。ジョブの終了通知を受けた端末は完了通知を発行し（ステップ５８）、完了通知の受領確認を受けて処理を終了する。

【００９４】

以上説明したような処理を行うことにより、本システムは、企業が管理する端末に対して自己のサービスを提供できるとともに、企業にとってはサーバ管理を事業主に委託することができ、低コストで幅広い多様なニーズに応えるサービスを提供できる。また、上記したように一般管理コンソールから管理できる端末は管理下にある端末のみであり、他の企業の管理下にある端末を管理することはできない。すなわち、自己の管理する端末を他企業のコンソールから管理されることはない。これにより、１つのＤＭＳを複数の企業で共用することができる。また、インターネットのように外部に開いたネットワークを用いても、本システムでは企業ＩＤのみならず管理者の認証を行うのでセキュリティ上も問題がない。

【００９５】

以上、本発明者によってなされた発明を発明の実施の形態に基づき具体的に説

明したが、本発明は前記実施の形態に限定されるものではなく、その要旨を逸脱しない範囲で種々変更可能であることは言うまでもない。たとえば、前記実施の形態ではエンドユーザである端末と企業の管理コンソールと事業者の特権管理コンソールの３階層の管理レベルを有するシステムを説明したが、より多階層の管理レベルが設定されても良い。たとえば事業者がその上層に位置する他の事業者に管理されてもよく、逆に企業に管理される端末がその管理範囲内で他の端末を管理するように構成されてもよい。

【００９６】

なお、本明細書では一般管理者の例として企業を示したが、官公庁、学校、団体その他のグループでも良い。本明細書において「企業」には、「官公庁、学校、団体その他のグループ」の概念も含む。

【００９７】

【発明の効果】

本願で開示される発明のうち、代表的なものによって得られる効果は、以下の通りである。すなわち、企業側に管理コンソールのみ設置して面倒な管理サーバの運用から企業を開放できる。ＩＳＰは有料で端末管理サービスを複数の企業に対して提供でき、企業側も経費を削減できる効果がある。

【００９８】

また、複数の企業が、同じ端末管理サーバやデータベース・サーバを共用して、自社の管理する端末に対してのみソフトウェア配布や端末設定などのサービスが行える。これにより、他社の管理する端末に対して端末設定などができないようにできる。

【００９９】

また、管理コンソールと管理サーバー間のセキュリティを強化して外部ネットワークを経由した管理コンソールが使用できる。

【図面の簡単な説明】

【図１】

本発明の一実施の形態であるネットワークシステムの概要を示した図である。

【図２】

本発明の一実施の形態であるシステムを機能に着目してさらに詳細に示した図である。

【図３】

コンソールマネージャ用のデータベース構造を示す図である。

【図４】

端末（デバイス）とサービスのグループ関係を示した図である。

【図５】

特権管理コンソールから端末管理サーバにリクエストを出し、サーバがこのリクエストに応える場合の処理の手順を示した図である。

【図６】

一般管理コンソールから端末管理サーバにリクエストを出し、サーバがこのリクエストに応える場合の処理の手順を示した図である。

【図７】

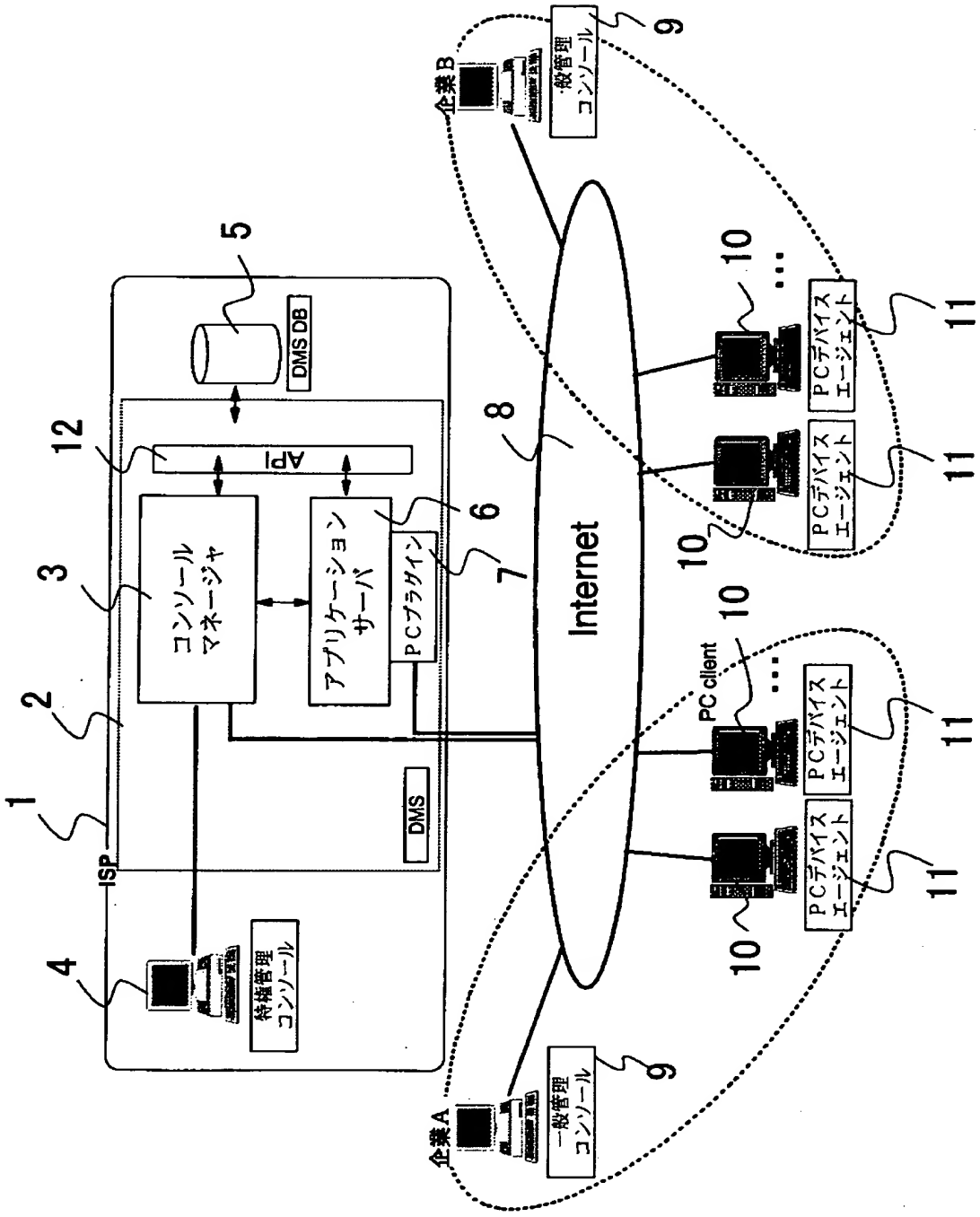
エンドユーザの端末から端末管理サーバにリクエストを出し、サーバがこのリクエストに応える場合の処理の手順を示した図である。

【符号の説明】

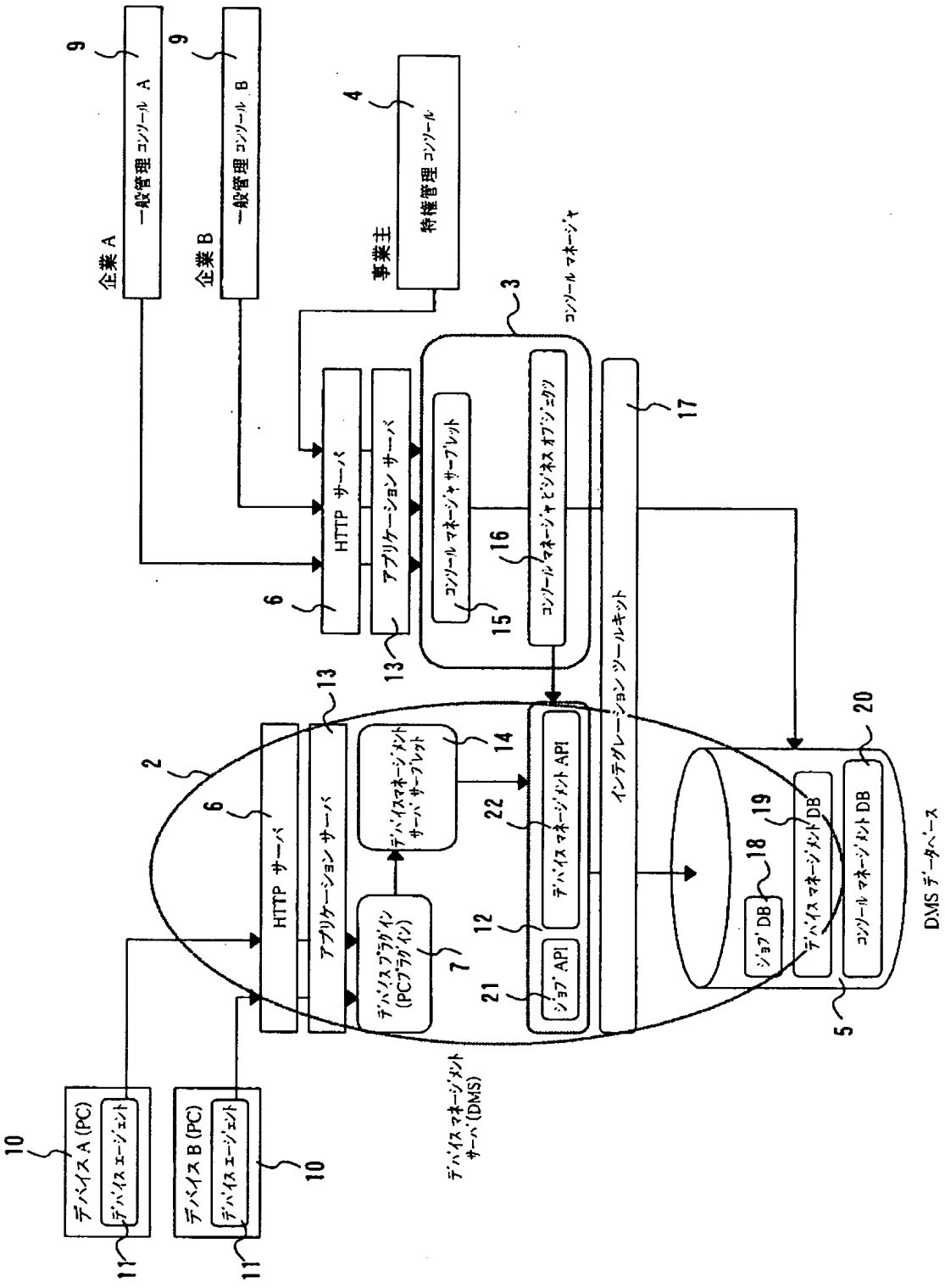
１…ＩＳＰ、２…端末管理サーバ、３…コンソール・マネージャ、４…特権管理コンソール、５…データベース、６…ＨＴＴＰサーバ、７…ＰＣプラグイン、８…インターネット、９…一般管理コンソール、１０…クライアント端末、１１…ＰＣデバイスエージェント、１２…ＡＰＩ、１３…アプリケーションサーバ、１４…デバイスマネージメントサーブレット、１６…コンソールマネージャビジネスオブジェクツ、１７…インテグレーションツールキット、１８…ジョブデータベース、１９…デバイスマネージメントデータベース、２０…コンソールマネージメントデータベース、３４…ENTERPRISEテーブル、３５…ADMINISTRATORテーブル、３７…企業追加リクエスト、４４…DEVICE_EXTテーブル。

【書類名】　　図面

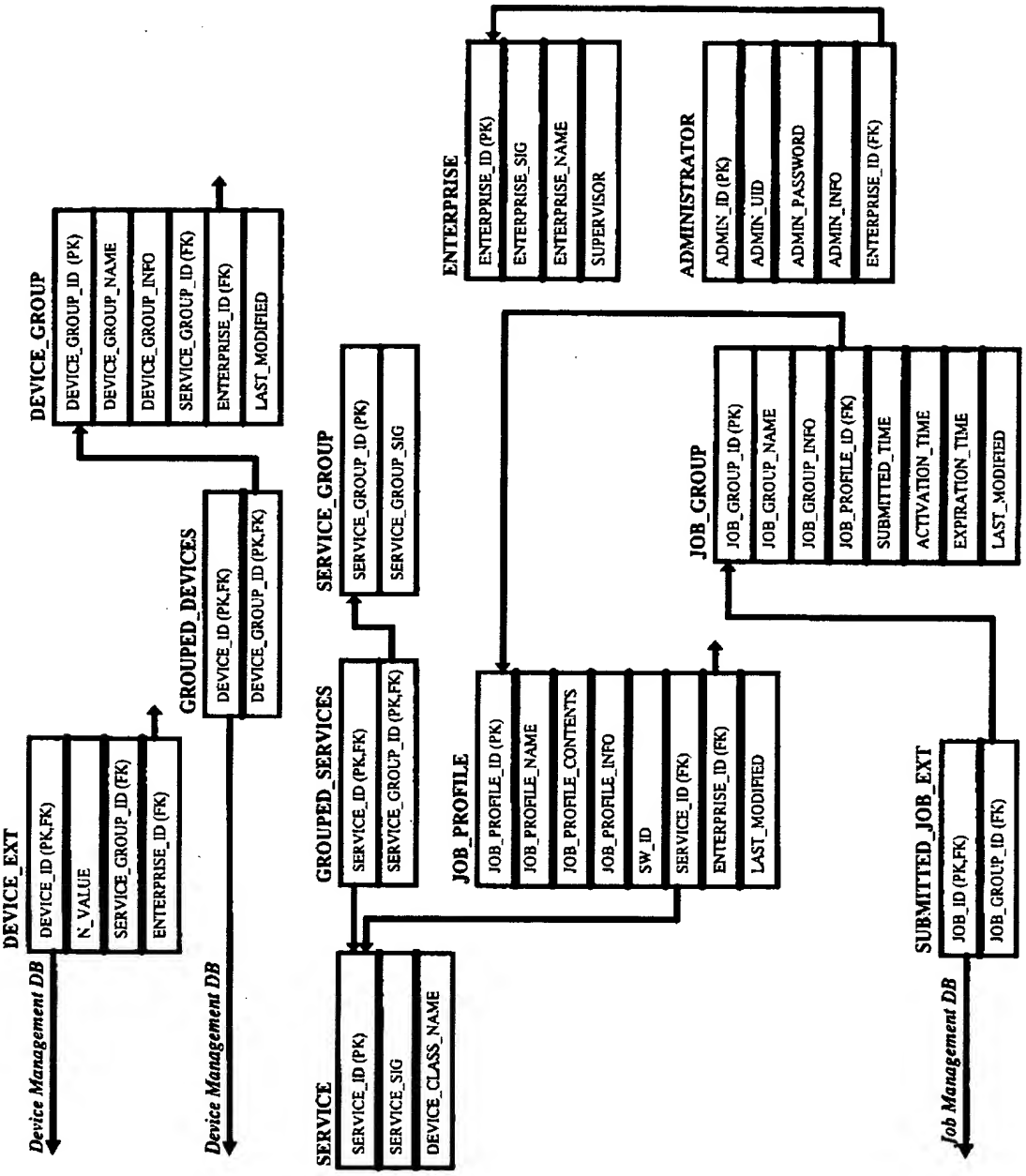
【図１】


1
2
3
4
5
6
7
8
9
10
11
12
ISP
コンソール
マネージャ
特権管理
コンソール
DMS DB
API
アプリケーション
サーバ
PCプラグイン
DMS
Internet
企業A
企業B
一般管理
コンソール
PC client
PCデバイス
エージェント

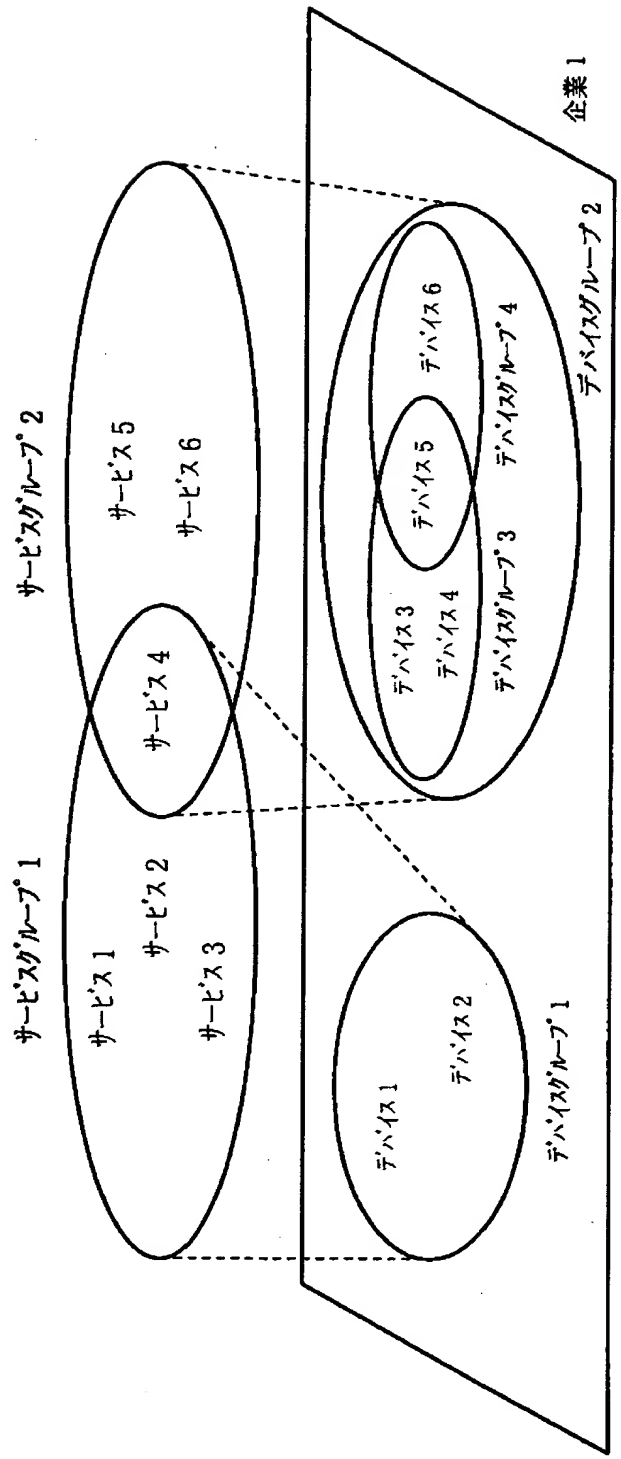
【図２】


企業A
一般管理コンソール A
9
企業B
一般管理コンソール B
9
事業主
特権管理コンソール
4
コンソール マネージャ
3
HTTP サーバ
6
アプリケーション サーバ
13
コンソール マネージャ サーブレット
15
コンソール マネージャ ビジネス オブジェクト
16
インテグレーション ツールキット
17
2
6
HTTP サーバ
13
アプリケーション サーバ
デバイス プラグイン (PCプラグイン)
7
デバイスマネージメント サーバ サーブレット
14
12
デバイス マネージメント API
22
ジョブ API
21
インテグレーション ツールキット
20
ジョブ DB
18
デバイス マネージメント DB
19
コンソール マネージメント DB
DMS データベース
5
デバイス マネージメント サーバ (DMS)
デバイス A (PC)
デバイス エージェント
10
11
デバイス B (PC)
デバイス エージェント
10
11

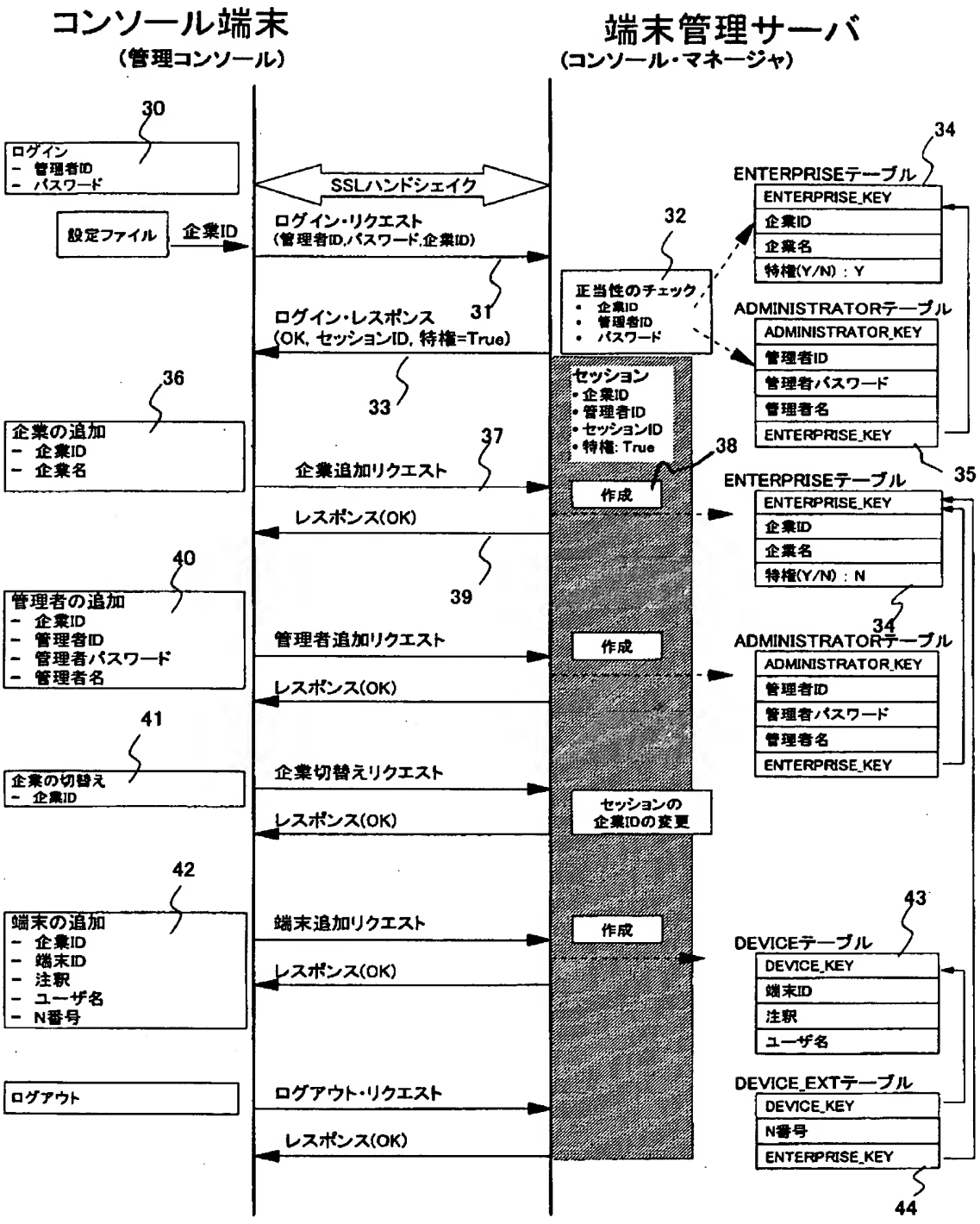
【図３】


ENTERPRISE
ENTERPRISE_ID (PK)
ENTERPRISE_SIG
ENTERPRISE_NAME
SUPERVISOR
ADMINISTRATOR
ADMIN_ID (PK)
ADMIN_UID
ADMIN_PASSWORD
ADMIN_INFO
ENTERPRISE_ID (FK)
DEVICE_GROUP
DEVICE_GROUP_ID (PK)
DEVICE_GROUP_NAME
DEVICE_GROUP_INFO
SERVICE_GROUP_ID (FK)
ENTERPRISE_ID (FK)
LAST_MODIFIED
SERVICE_GROUP
SERVICE_GROUP_ID (PK)
SERVICE_GROUP_SIG
JOB_GROUP
JOB_GROUP_ID (PK)
JOB_GROUP_NAME
JOB_GROUP_INFO
JOB_PROFILE_ID (FK)
SUBMITTED_TIME
ACTIVATION_TIME
EXPIRATION_TIME
LAST_MODIFIED
GROUPED_DEVICES
DEVICE_ID (PK,FK)
DEVICE_GROUP_ID (PK,FK)
GROUPED_SERVICES
SERVICE_ID (PK,FK)
SERVICE_GROUP_ID (PK,FK)
JOB_PROFILE
JOB_PROFILE_ID (PK)
JOB_PROFILE_NAME
JOB_PROFILE_CONTENTS
JOB_PROFILE_INFO
SW_ID
SERVICE_ID (FK)
ENTERPRISE_ID (FK)
LAST_MODIFIED
DEVICE_EXT
DEVICE_ID (PK,FK)
N_VALUE
SERVICE_GROUP_ID (FK)
ENTERPRISE_ID (FK)
SUBMITTED_JOB_EXT
JOB_ID (PK,FK)
JOB_GROUP_ID (FK)
SERVICE
SERVICE_ID (PK)
SERVICE_SIG
DEVICE_CLASS_NAME
Device Management DB
Device Management DB
Job Management DB

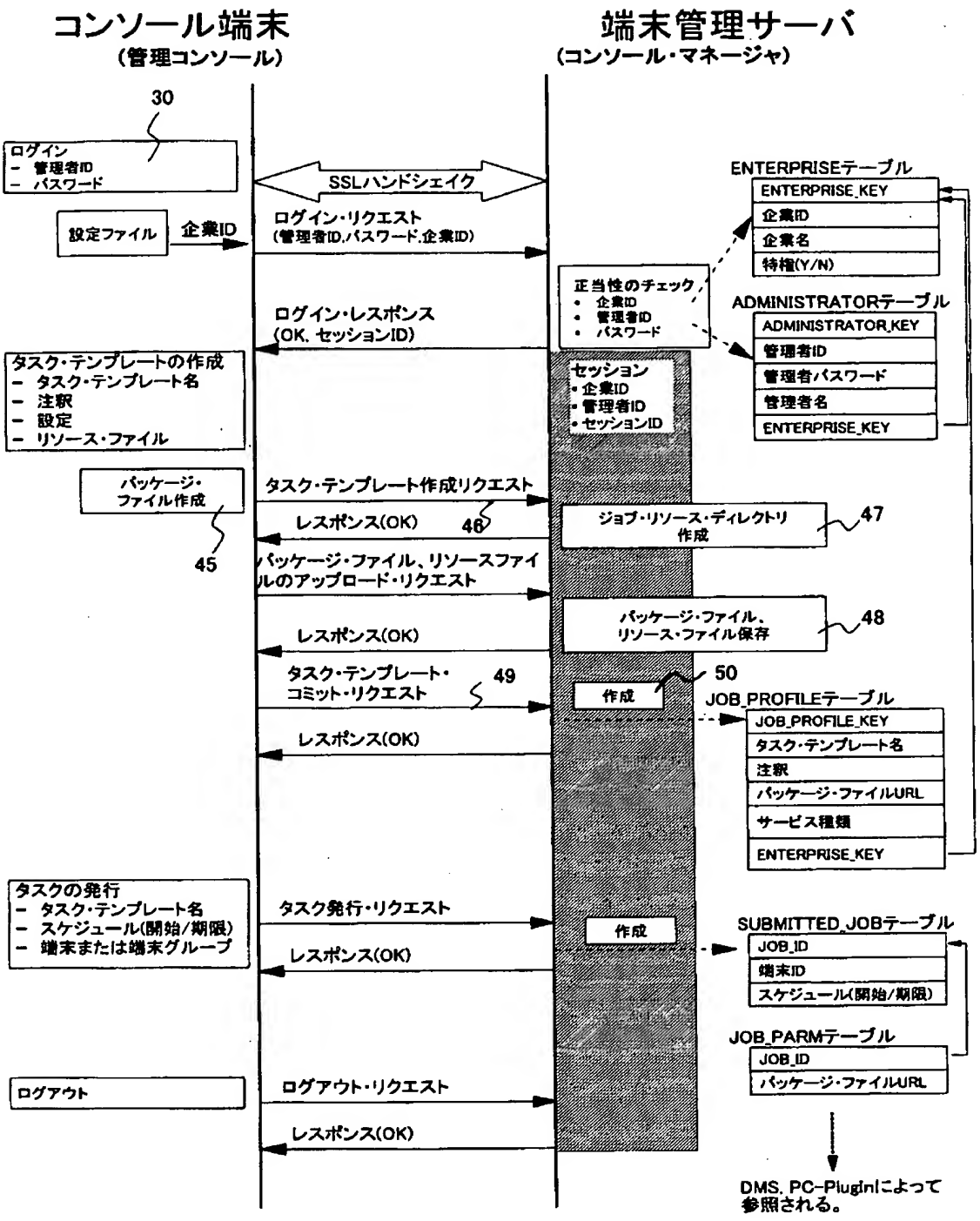
【図４】


企業１
サービスグループ２
サービス５
サービス６
サービス４
サービスグループ１
サービス１
サービス２
サービス３
デバイスグループ２
デバイス６
デバイス５
デバイス４
デバイス３
デバイスグループ４
デバイスグループ３
デバイス１
デバイス２
デバイスグループ１

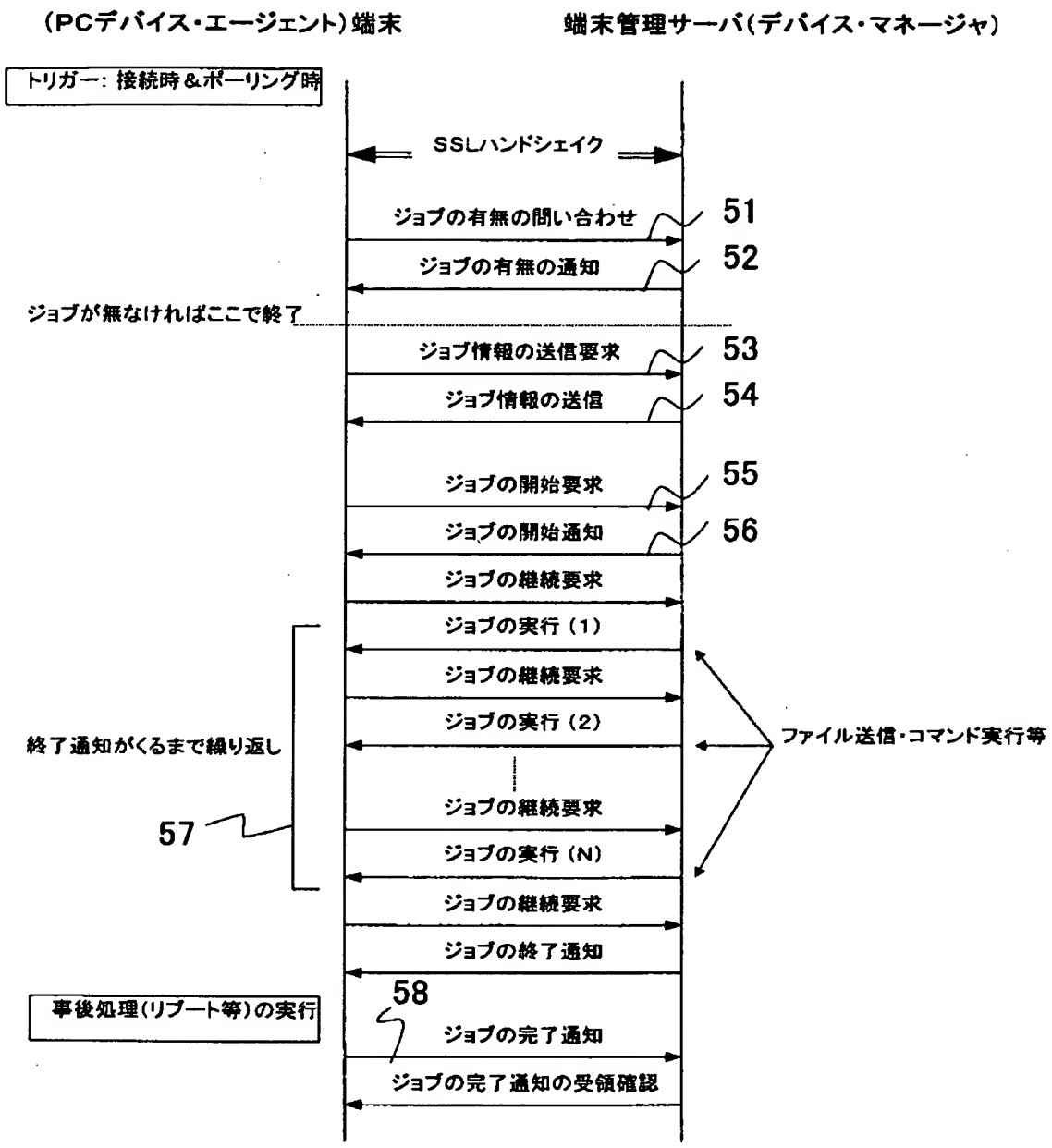
【図５】


コンソール端末
（管理コンソール）
端末管理サーバ
（コンソール・マネージャ）
30
ログイン
- 管理者ID
- パスワード
SSLハンドシェイク
設定ファイル
企業ID
ログイン・リクエスト
（管理者ID,パスワード,企業ID）
32
正当性のチェック
• 企業ID
• 管理者ID
• パスワード
31
ログイン・レスポンス
（OK, セッションID, 特権=True）
33
セッション
• 企業ID
• 管理者ID
• セッションID
• 特権: True
34
ENTERPRISEテーブル
ENTERPRISE_KEY
企業ID
企業名
特権(Y/N) : Y
ADMINISTRATORテーブル
ADMINISTRATOR_KEY
管理者ID
管理者パスワード
管理者名
ENTERPRISE_KEY
35
36
企業の追加
- 企業ID
- 企業名
37
企業追加リクエスト
38
作成
ENTERPRISEテーブル
ENTERPRISE_KEY
企業ID
企業名
特権(Y/N) : N
レスポンス(OK)
39
34
40
管理者の追加
- 企業ID
- 管理者ID
- 管理者パスワード
- 管理者名
管理者追加リクエスト
作成
ADMINISTRATORテーブル
ADMINISTRATOR_KEY
管理者ID
管理者パスワード
管理者名
ENTERPRISE_KEY
レスポンス(OK)
41
企業の切替え
- 企業ID
企業切替えリクエスト
セッションの
企業IDの変更
レスポンス(OK)
42
端末の追加
- 企業ID
- 端末ID
- 注釈
- ユーザ名
- N番号
端末追加リクエスト
作成
43
DEVICEテーブル
DEVICE_KEY
端末ID
注釈
ユーザ名
レスポンス(OK)
ログアウト
ログアウト・リクエスト
DEVICE_EXTテーブル
DEVICE_KEY
N番号
ENTERPRISE_KEY
レスポンス(OK)
44

【図６】


コンソール端末
（管理コンソール）
端末管理サーバ
（コンソール・マネージャ）
30
ログイン
－ 管理者ID
－ パスワード
SSLハンドシェイク
ENTERPRISEテーブル
ENTERPRISE_KEY
企業ID
企業名
特権(Y/N)
設定ファイル
企業ID
ログイン・リクエスト
（管理者ID,パスワード,企業ID）
正当性のチェック
• 企業ID
• 管理者ID
• パスワード
ADMINISTRATORテーブル
ADMINISTRATOR_KEY
管理者ID
管理者パスワード
管理者名
ENTERPRISE_KEY
ログイン・レスポンス
（OK, セッションID）
セッション
• 企業ID
• 管理者ID
• セッションID
タスク・テンプレートの作成
－ タスク・テンプレート名
－ 注釈
－ 設定
－ リソース・ファイル
パッケージ・
ファイル作成
45
タスク・テンプレート作成リクエスト
レスポンス(OK)
46
ジョブ・リソース・ディレクトリ
作成
47
パッケージ・ファイル、リソースファイ
ルのアップロード・リクエスト
パッケージ・ファイル、
リソース・ファイル保存
48
レスポンス(OK)
タスク・テンプレート・
コミット・リクエスト
49
作成
50
JOB_PROFILEテーブル
JOB_PROFILE_KEY
タスク・テンプレート名
注釈
パッケージ・ファイルURL
サービス種類
ENTERPRISE_KEY
レスポンス(OK)
タスクの発行
－ タスク・テンプレート名
－ スケジュール(開始/期限)
－ 端末または端末グループ
タスク発行・リクエスト
作成
SUBMITTED_JOBテーブル
JOB_ID
端末ID
スケジュール(開始/期限)
レスポンス(OK)
JOB_PARMテーブル
JOB_ID
パッケージ・ファイルURL
ログアウト
ログアウト・リクエスト
レスポンス(OK)
DMS, PC-PlugInによって
参照される。

【図７】


(PCデバイス・エージェント)端末
端末管理サーバ(デバイス・マネージャ)
トリガー：接続時＆ポーリング時
SSLハンドシェイク
ジョブの有無の問い合わせ
51
ジョブの有無の通知
52
ジョブが無ければここで終了
ジョブ情報の送信要求
53
ジョブ情報の送信
54
ジョブの開始要求
55
ジョブの開始通知
56
ジョブの継続要求
ジョブの実行（1）
ジョブの継続要求
ジョブの実行（2）
終了通知がくるまで繰り返し
ファイル送信・コマンド実行等
ジョブの継続要求
57
ジョブの実行（N）
ジョブの継続要求
ジョブの終了通知
58
事後処理(リブート等)の実行
ジョブの完了通知
ジョブの完了通知の受領確認

【書類名】　　要約書

【要約】

【課題】　企業側に管理コンソールのみ設置して面倒な管理サーバの運用から企業を開放する。ＩＳＰは有料で端末管理サービスを複数の企業に対して提供し、企業側も経費を削減できるようにする。

【解決手段】　インターネット８に接続された一般管理コンソール９と、サーバ２にアクセス可能な特権管理コンソール４と、端末管理サーバ２に接続されたデータベース５と、データ処理を仲介するコンソールマネージャ３と、を有し、データベース５には、一般管理コンソール９毎に関連付けられている企業データ、企業データに関連付けられている端末１０毎の端末データ、を含み、企業データと端末データとを参照して、関連付けられている端末またはそのグループに対するサービスの提供を関連付けられている一般管理コンソールに対して許可する手段を含む。

【選択図】　図１

認定・付加情報

特許出願の番号	特願２０００－２０７５８７
受付番号	５００００８６０８２５
書類名	特許願
担当官	濱谷　よし子　　１６１４
作成日	平成１２年　８月２２日

＜認定情報・付加情報＞

【特許出願人】

【識別番号】　390009531

【住所又は居所】　アメリカ合衆国１０５０４、ニューヨーク州　アーモンク　（番地なし）

【氏名又は名称】　インターナショナル・ビジネス・マシーンズ・コーポレーション

【代理人】

【識別番号】　100086243

【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　大和事業所内

【氏名又は名称】　坂口　博

【復代理人】　申請人

【識別番号】　100112520

【住所又は居所】　神奈川県大和市中央林間３丁目４番４号　サクライビル４階　間山・林合同技術特許事務所

【氏名又は名称】　林　茂則

【選任した代理人】

【識別番号】　100091568

【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　大和事業所内

【氏名又は名称】　市位　嘉宏

【選任した代理人】

【識別番号】　100106699

【住所又は居所】　神奈川県大和市下鶴間１６２３番１４　日本アイ・ビー・エム株式会社大和事業所内

【氏名又は名称】　渡部　弘道

【選任した復代理人】

【識別番号】　100110607

次頁有

認定・付加情報（続き）

【住所又は居所】　神奈川県大和市中央林間３丁目４番４号　サクライビル４階　間山・林合同技術特許事務所
【氏名又は名称】　間山　進也
【選任した復代理人】
【識別番号】　100098121
【住所又は居所】　神奈川県大和市中央林間３丁目４番４号　サクライビル４階　間山・林合同技術特許事務所
【氏名又は名称】　間山　世津子

次頁無

出　願　人　履　歴　情　報

識別番号　　〔３９０００９５３１〕

１．変更年月日　　２０００年　５月１６日
［変更理由］　名称変更
住　所　　アメリカ合衆国１０５０４、ニューヨーク州　アーモンク　（番地なし）
氏　名　　インターナショナル・ビジネス・マシーンズ・コーポレーション